IN THE DRAWINGS:

The drawings were objected to as containing multiple figures that are handwritten and contain sloppy text. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are attached to this response. As such, Applicant respectfully requests that the objection be withdrawn.

REMARKS

Claims 1, 4, 6, 8-12, 15, 17, and 19-21 stand rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Ahonen (U.S. patent No. 6,976,177). Applicant respectfully traverses this rejection.

As to claim 1, contrary to what is stated in the Office Action, Ahonen fails to teach or suggest "establishing a correspondence between the IP address and a first shared secret authorized for the user," "receiving a second request from the user to form a virtual private network tunnel, the request incorporating a second shared secret," "determining whether the first shared secret matches the second shared secret," or "forming the virtual private network tunnel when the first shared secret matches the second shared secret." Specifically, Ahonen fails to teach or suggest the use of a shared secret at all, let alone the specific uses of the shared secret described in claim 1. Ahonen utilizes digital certificates. This can be seen from, for example, col. 9, lines 52-61 of Ahonen ("The firewall 3 receives the control authorisation certificate. This input is compared with the contents of the RCDB within the firewall 3. The firewall 3 identifies whether or not any record in RCDB for this mobile host 1 matches with the three corresponding input fields received in the control certificate....").

The drawbacks of utilizing digital certificates for VPN authorization are described in the Specification of the present application, page 2, line 30 through page 3, line 2. Specifically, "[d]igital certificates require a substantial amount of infrastructure, including the involvement of a third-party certification authority. The complexity and expense of this involvement make the use of digital certificates less than optimal for, e.g., forming a VPN tunnel to a home network." Ahonen's use of the digital certificates is in contrast to the claimed invention, which utilizes a shared secret. As such, Ahonen fails to teach or suggest the above-identified elements of claim 1. Therefore, Applicant respectfully maintains that claim 1 is in condition for allowance.

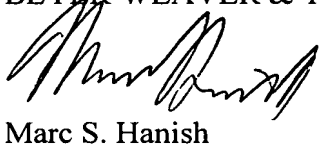
As to independent claims 12, 19, and 20 contain elements similar to that as described above with respect to claim 1. As such, Applicant respectfully maintains that these claims are also in condition for allowance.

As to independent claim 21, this claim has been canceled without prejudice or disclaimer.

As to dependent claims 4, 6, 8-11, 15, and 17, since these claims are dependent claims, they are allowable for the same reasons as the independent claims from which they depend.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP



Marc S. Hanish
Reg. No. 42,626

P.O. Box 70250
Oakland, CA 94612-0250
650-961-8300